What is claimed is:

1. A countermeasure method in an electronic component using a public key cryptography algorithm based on the use of elliptic curves in which a private key d and the number of points n on an elliptic curve are used to calculate a new deciphering integer d′ such that the deciphering of any message, by means of a deciphering algorithm, with d′ makes it possible to obtain the same result as with d, by performing the operation Q=d.P, where P is a point on the curve to which the scalar multiplication algorithm is applied, said method comprising the following steps:

1) taking a random value r with the same size as d;

2) calculating an integer d′ such that d′=d+r;

3) Performing a scalar multiplication operation whose result is a point Q′ on the curve such that Q′=d′.P;

4) Performing a scalar multiplication operation whose result is a point S on the curve such that S=r.P; and

5) calculating the point Q on the curve such that Q=Q′-S.

2. A countermeasure method according to Claim 1, wherein a new deciphering integer d′ is calculated at each new execution of the deciphering algorithm.

3. A countermeasure method according to Claim 1, further including the step of incrementing a counter at each new execution of the deciphering algorithm up to an integer value T.

4. A countermeasure method according to Claim 3, wherein once the value T has been reached, a new deciphering integer d′ is calculated

according to the method of Claim 1, the counter is reset to zero and the point $S=r.P$ is stored in memory.

5. A countermeasure method according to Claim 4 wherein the value T is equal to 16.

6. A countermeasure method according to Claim 3 wherein the value T is equal to 16.

7. A countermeasure method according to Claim 1, wherein the point S is stored in memory, and steps 1 and 4 are replaced by the following steps 1′ and 4′:

1′) replace r by 2.r

4′) replace S by 2.S.

8. A countermeasure method according to Claim 7, wherein a new deciphering integer d' is calculated at each new execution of the deciphering algorithm.

9. A countermeasure method according to Claim 7, further including the step of incrementing a counter at each new execution of the deciphering algorithm up to a value T.

10. A countermeasure method according to Claim 9, wherein, once the value T has been reached, a new deciphering integer d' is calculated according to the method of Claim 7, and the counter is reset to zero.

11. A countermeasure method according to Claim 10 wherein the value T is equal to 16.

12. A countermeasure method according to Claim 10 wherein the value T is equal to 16.

13. An electronic component having an integrated circuit which executes a public key cryptography algorithm based on the use of elliptic curves in which a private key d and the number of points n on an elliptic curve are used to calculate a new deciphering integer d′ such that the deciphering of any message, by means of a deciphering algorithm, with d′ makes it possible to obtain the same result as with d, by performing the operation Q=d.P, where P is a point on the curve to which the scalar multiplication algorithm is applied, said circuit executing the following steps:

1) taking a random value r with the same size as d;

2) calculating an integer d′ such that d′=d+r;

3) Performing a scalar multiplication operation whose result is a point Q′ on the curve such that Q′=d′.P;

4) Performing a scalar multiplication operation whose result is a point S on the curve such that S=r.P; and

5) calculating the point Q on the curve such that Q=Q′-S.